PATENT APPLICATION

ATTORNEY DOCKET NO. ___10992881-1___

JUN 1 5 2005

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):   Cormac Herley

Application No.: 09/776,680

Filing Date: Feb. 6, 2005

Title: Method And Apparatus For Partial
Encryption Of Content

Confirmation No.: 2533

Examiner: Beemnet Dada

Group Art Unit: 2135

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on **April 15, 2005**   .

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

( ) (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

( )	one month	$120.00
( )	two months	$450.00
( )	three months	$1020.00
( )	four months	$1590.00

06/16/2005 SZEWDIE1 00000013 082025   09776680
01 FC:1402   500.00 DA

( ) The extension fee has already been filled in this application.

( ) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account **08-2025** the sum of ___**$500.00**___. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

Date: ___June 15, 2005___

I hereby certify that this document is being filed by personal delivery to the Customer Service Window Randolph Building, 401 Dulany Street Alexandria, VA 22314, of the United States Patent & Trademark Office on the date indicated above.

By: _____ Reg No 32,858
(Attorney Signature and Reg. No.)

Respectfully submitted,

Cormac Herley

By _____

Patrick C. Keane

Attorney/Agent for Applicant(s)
Reg. No.   **32,858**

Date: **June 15, 2005**

Rev 12/04 (Aplbrief)

Telephone No.: **(703) 838-6522**

I.   Real Party in Interest

The present application is assigned to Hewlett Packard Development Company L.P.

II.   Related Appeals and Interferences

The Appellant's legal representative, or assignee, does not know of any other appeal or interferences which will affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

III.   Status of Claims

Claims 2-7 and 13-14 and 16-20 remain pending in the application. Claims 1, 8-12 and 15 have been canceled. Claims 6 and 16 are the sole independent claims pending in the application.

IV.   Status of Amendments

An Amendment After Final was filed February 22, 2005. Entry of this Amendment is requested for purposes of this Appeal, pursuant the Examiner's indication in paragraph 7 of the Advisory Action dated March 15, 2005.

V.   Summary of Claimed Subject Matter

Appellants' specification describes methods and apparatus for partially encrypting an information file, such as a data file of text and/or image information, for secure delivery of content. As described at specification page 4, lines 13-19, exemplary embodiments are directed to the secure delivery of an information file which has been divided into at least two separate files; i.e., a first file and a second file. As described at specification page 5, lines 14-18, use limitations are added to

the information file to prevent the second file from being used more than an authorized number of times. See also, for example, step 220 in Figure 2. As such, the second file can only be used by recipients in a manner prescribed by the use limitations.

In Figure 3, an exemplary information file such as the image file (such as a work of art), 300 is divided into a first file 310 and a second file 320 as described at specification page 6, lines 8-22. The second file 320 is encrypted using a desired encryption system. The first file and the encrypted second file can be transmitted to a secure device 360 via a communication path 330, such as the Internet. The secure device 360 can decrypt the second file and combine it with the first file to reconstruct a usable version of the original file 300 as a reconstructed image file 340.

In dividing the information file, enough content of the original file is extracted to render the first file inadequate to sufficiently reconstruct the original information file using only the first file. Figure 4 shows an exemplary method for dividing an image via a user selected pattern. In Figure 4, the user selected pattern 430 is applied to an image file 410, for example as an overlay, to extract content used to form the second file 420 as described at specification page 7, lines 17-21.

The foregoing features are encompassed by independent claims 6 and 16, and are neither taught nor suggested by the documents relied upon by the Examiner.

VI.   Grounds of Rejection to be Reviewed on Appeal

In numbered paragraph 13 on page 5 of the Final Office Action, claims 6-7 and 16-17 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,999,622 (Yasukawa) in view of EP document 0 614 308 A1 (Melnychuck). Following entry of the Amendment After Final, all of the remaining

pending claims 2-5, 13-14 and 18-20 now depend from claims 6 and 16, making this the sole rejection to be reviewed on appeal.

VII.   Argument

      A.   The Examiner Has Failed To Establish A Prima Facie Case Of Obviousness In Rejecting Appellants' Claims Over A Combination Of The Yasukawa And Melnychuck Documents

Appellants' independent claims 6 and 16 are allowable over the Yasukawa and Melnychuck documents. The Yasukawa document, considered alone or in combination with the Melnychuck document, fails to teach or suggest Applicants' invention as presently set forth in independent claims 6 and 16.

For example, Claim 6 recites:

A method of partially encrypting an information file for delivery of content comprising:
dividing an information file into a first file and a second file, wherein the second file includes content from the information file to preclude reconstruction of the information file using only the first file, and wherein use limitations are included with the information file to prevent use of the second file to reconstruct the information file more than an authorized number of times; and
encrypting the second file, wherein dividing the information file comprises:
selecting parts from the information file via a user selected pattern.

Claim 16 is a system which includes elements for performing functions similar to those of claim 6.

The Yasukawa patent is directed to protecting widely distributed digital information by segmenting each file. See the Title and Abstract of the Yasukawa patent. Each segment (e.g., disk sector) of each file is encrypted separately. As also described in the Abstract of the Yasukawa patent, some segments can be left

unencrypted, and different segments can be encrypted using different encryption

techniques.

The Melnychuck document was cited by the Examiner on page 5 of the Final

Office Action with respect to claims 6-7 and 16-17, and with respect to all presently

pending claims in the March 15, 2005 Advisory Action. On page 5 of the Final Office

Action, the Examiner states:

> Yasukawa does not explicitly teach dividing the information file comprising
> selecting parts from the information file via a user selected pattern. However,
> within the same field of endeavor Melnychuck teaches a partial encryption
> method including, user selecting parts section of the file [column 1, lines 40-
> 57]. Therefore, it would have been obvious to one having ordinary skill in the
> art at the time the invention was made to include a user selection method for
> selecting parts from the information file as taught by Melnychuck into the
> system of Yasukawa, because the modification further allows selection of a
> file segment based on a user's interest.

In numbered paragraph 11 of the March 15th Advisory Action, the Examiner

states:

> Claims 6 and 16 are rejected [over] Yasukawa in view of Melnychuck.
> Applicant argues that the Melnychuck patent fails to teach providing user
> selected pattern for selecting parts from an information file to be encrypted.
> The examiner respectfully disagrees. Melnychuck (EP 0614308 A1) discloses
> encryption of selected image component of an image hierarchy, where parts
> of an image component are encrypted, further including user selection means
> for selecting an image component [see Melnychuck, column 1, lines 34-57],
> which meets the claimed recitation. Yasukawa (US Patent No. 5,999,622)
> teaches dividing an information file into a first file and a second file (non-
> encrypted section and encrypted section [claim 3, lines 53-65 and column 4,
> lines 16-21], wherein the second file includes content from the information file
> to preclude reconstruction of the information file using only first file [column 3,
> lines 53-65], and encrypting the second file [column 3, lines 53-65 and column
> 4, lines 16-21], and encrypting the second file [column 4, lines 16-21].
> Modification of Melnychuck within Yasukawa meets the claimed invention.
> Therefore the rejection is respectfully maintained.

The assertions that the Melnychuck and Yasukawa documents disclose or suggest Appellants' presently claimed invention are respectfully traversed. The Melnychuck document is directed to image processing using a method which allows for restriction of access to image components in a hierarchical storage and retrieval system. As described in the Abstract of the Melnychuck document, the disclosed technique employs a key encryption of selected image components during storage, and decryption with a special key, or password during authorized retrieval.

As described at column 1, lines 40-57 of the Melnychuck document, an image of compromised (i.e., lesser) image quality can be delivered for purposes of browsing or proofing. For example, the Melnychuck document states that when a user selects an image from a catalog of images depicting a particular object, the user can browse the relatively low resolution images. As described earlier in column 1 (e.g., column 1, lines 21 et seq.), an original image is decomposed to provide image versions of various resolutions, thereby providing an image hierarchy.

Thus, an entire image can be reconstructed at a lower resolution using the system of Melnychuck. Use of a high resolution component for purposes of producing a full image quality can be restricted, as described, for example, at column 2, lines 35-54. This portion of the Melnychuck patent states that an authorization code, key or password can be provided to a user to "unlock" restricted high resolution components stored in a digital storage medium.

There would have been no motivation or suggestion to have combined features from the Yasukawa and Melnychuck documents in the manner suggested by the Examiner to arrive at the presently claimed invention. It is unclear from the documents cited why one skilled in the art would have been motivated to pick and

choose features from the two cited documents in such a manner as to arrive at the presently claimed invention. As such, the Examiner has failed to establish a *prima facie* case of obviousness.

Moreover, even if features of these two documents could have been combined in the manner suggested by the Examiner, the presently claimed invention would not have resulted. For example, neither of the documents relied upon by the Examiner teach or suggest providing a "user selected pattern" for selecting parts from an information file to be encrypted, as recited in Appellants' independent claims 6 and 16.

The Yasukawa patent, as recognized by the Examiner, does not teach or suggest such a feature. The Melnychuck patent is merely directed to providing an image at different resolutions, and for storing different components of an image in a digital storage medium at user location for access by the user via a code, key or password. Neither Yasakuwa nor Melnychuck teach or suggest encrypting a second file which has been selected via a user selected pattern, such as that shown in Appellants' Figure 3 and encompassed by Appellants' claim 6. The cited portion of the Melnychuck document (i.e., column 1, lines 34-57) does not disclose or suggest use of a "user selected pattern" such as would be used with the work of art illustrated in Appellants' Figure 3. This portion of the Melnychuck document constitutes a background of the Melnychuck disclosure and merely refers to a "user-defined criterion" associated with a "browsing" function used to select an image from among a catalog of images (see column 1, lines 45-50). As such, claim 6 is allowable. Claim 16 recites similar features, and is also allowable.

All of the remaining claims depend from the aforementioned independent claims and are similarly allowable, such that reversal of the Examiner's rejection in the Final Office Action is requested.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix
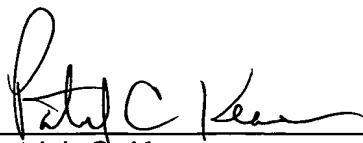
NONE

X. Related Proceedings Appendix

NONE

XI CONCLUSION

Reversal of the Examiner's final rejection is respectfully requested, and a Notice of Allowance is solicited.

Respectfully submitted,

Burns, Doane, Swecker & Mathis, L.L.P.

Date ___June 15, 2005___   By: _____

Patrick C. Keane
Registration No. 32,858

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Table of Contents

VIII. CLAIMS APPENDIX

The Appealed Claims

1. (Canceled)

2. (Previously Presented) The method of claim 6, further comprising:
transmitting the first file and the encrypted second file to a device.

3. (Original) The method of claim 2, wherein the first file and the encrypted second file are transmitted via the Internet.

4. (Previously Presented) The method of claim 6, wherein the step of encrypting includes:
using an RSA algorithm.

5. (Previously Presented) The method of claim 6, comprising:
adding the use limitations to the second file.

6. (Previously Presented) A method of partially encrypting an information file for delivery of content comprising:
dividing an information file into a first file and a second file, wherein the second file includes content from the information file to preclude reconstruction of the information file using only the first file, and wherein use limitations are included with the information file to prevent use of the second file to reconstruct the information file more than an authorized number of times; and
encrypting the second file, wherein dividing the information file comprises:
selecting parts from the information file via a user selected pattern.

7. (Previously Presented) The method of claim 6, wherein dividing the information file comprises:
selecting parts from the information file via a default pattern related to content contained in the information file, to form the second file.

8. (Canceled) .

Claims Appendix - 1

9.   (Canceled)

10.   (Canceled)

11.   (Canceled)

12.   (Canceled)

13.   (Previously Presented) The system of claim 16, wherein the communication path is the Internet.

14.   (Previously Presented) The method of claim 16, wherein the second file is encrypted using a RSA algorithm.

15.   (Canceled)

16.   (Previously Presented) A system for partially encrypting an information file for delivery comprising:

a server that divides an information file into a first file and a second file, wherein the second file includes content from the information file to preclude reconstruction of the information file using only the first file, and that encrypts the second file, and wherein use limitations are included with the information file to prevent use of the second file to reconstruct the information file more than an authorized number of times;

a device that receives the first file and the encrypted second file, that decrypts the second file, and that combines the first file and the decrypted second file to reconstruct a usable version of the information file; and

a communication path that operably interconnects the server and the device wherein the server comprises:

logic that includes the use limitations with encryption of the second file, wherein the server comprises:

logic that selects parts from the information file that form the second file via a user selected pattern.

17.   (Previously Presented) The system of claim 16, wherein the server comprises:

logic that selects parts from the information file that form the second file via a default pattern related to the content contained in the information file.

18.   (Previously Presented) The system of claim 16, wherein the device is at least one of a personal computer, a printer and a digital appliance.

19.   (Previously Presented) The system of claim 16, wherein the device is a printer which includes an embedded private key needed to decrypt the second file and print the information file.

20.   (Previously Presented) The method of claim 2, wherein the device is a printer which includes an embedded private key needed to decrypt the second file and print the information file.

IX. EVIDENCE APPENDIX

NONE

X. RELATED PROCEEDINGS APPENDIX

NONE